BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problems Mailbox.

Docket No. 208915US2RD/vdm

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Masahiro TAKAGI, et al. GAU: 2661

SERIAL NO: 09/862,440 EXAMINER:

FILED: May 23, 2001

FOR: COMMUNICATION CONTROL SCHEME USING PROXY DEVICE AND SECURITY PROTOCOL IN COMBINATION

REQUEST FOR PRIORITY

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number [US App No], filed [US App Dt], is claimed pursuant to the provisions of **35 U.S.C. §120**.
- ☐ Full benefit of the filing date of U.S. Provisional Application Serial Number , filed , is claimed pursuant to the provisions of **35 U.S.C. §119(e)**.
- ■ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of **35 U.S.C. §119**, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY	APPLICATION NUMBER	MONTH/DAY/YEAR
JAPAN	2000-151434	May 23, 2000

Certified copies of the corresponding Convention Application(s)

- ■ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. filed
- ☐ were submitted to the International Bureau in PCT Application Number .
  Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and
  (B) Application Serial No.(s)
  - ☐ are submitted herewith
  - ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Joseph A. Scafetta Jr.

Marvin J. Spivak
Registration No. 24,913

Joseph A. Scafetta, Jr.
Registration No. 26,803

22850
Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 10/98)

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２０００年　５月２３日

出願番号
Application Number: 特願２０００－１５１４３４

出願人
Applicant(s): 株式会社東芝

２００１年　５月３０日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

出証番号　出証特２００１－３０４７４１６

【書類名】　特許願

【整理番号】　13B0050291

【提出日】　平成12年 5月23日

【あて先】　特許庁長官殿

【国際特許分類】　H04L 12/66

H04B 7/26

H04Q 7/22

【発明の名称】　ゲートウェイ装置、通信装置、制御装置、および通信制御方法

【請求項の数】　12

【発明者】

【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

【氏名】　高木　雅裕

【発明者】

【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

【氏名】　石山　政浩

【特許出願人】

【識別番号】　000003078

【氏名又は名称】　株式会社　東芝

【代理人】

【識別番号】　100081732

【弁理士】

【氏名又は名称】　大胡　典夫

【選任した代理人】

【識別番号】　100075683

【弁理士】

【氏名又は名称】　竹花　喜久男

【選任した代理人】

【識別番号】　100084515

【弁理士】

【氏名又は名称】　宇治　弘

【手数料の表示】

【予納台帳番号】　009427

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　0001435

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　ゲートウェイ装置、通信装置、制御装置、および通信制御方法

【特許請求の範囲】

【請求項１】

無線網に収容された無線端末装置と有線網に収容された有線端末装置との間でトランスポート層以上の情報の中継を行うゲートウェイ装置において、

前記無線端末装置と前記有線端末装置との間で秘匿性を保証する通信のために、前記無線端末装置と前記有線端末装置との間に設定される第１のセキュリティアソシエーションに関する情報を保持する第１のセキュリティ情報保持手段と、

前記無線端末装置と前記有線端末装置との間で秘匿性を保証する通信を中継する際に前記第１セキュリティアソシエーションに関する情報を利用して前記無線端末装置もしくは前記有線端末装置に受信される暗号化された情報を復号化する情報復号化手段と、

前記復号化された情報に基づいて前記トランスポート層以上の情報を利用して中継処理を行う中継手段と、

前記中継手段が送信する情報を前記第１のセキュリティアソシエーションに関する情報を利用して秘匿化する情報暗号化手段と

を具備したことを特徴とするゲートウェイ装置。

【請求項２】

無線網に収容された無線端末装置と有線網に収容された有線端末装置との間でトランスポート層以上の情報の中継を行うゲートウェイ装置において、

前記無線端末装置と前記有線端末装置との間で情報の認証を保証した通信を行うために、前記無線端末装置と前記有線端末装置との間に設定される第１のセキュリティアソシエーションに関する情報を保持する第１のセキュリティ情報保持手段と、

前記無線端末装置と前記有線端末装置との間で前記認証を保証された情報を前記トランスポート層以上の情報を利用して中継処理を行う中継手段と、

前記中継手段が中継する前記認証が保証された情報および前記中継手段が必要に応じて新たに生成した情報に対して前記第１のセキュリティアソシエーション

に関する情報を利用して、前記認証が保証された情報を保証する認証情報を付加する認証情報手段と
を具備したことを特徴とするゲートウェイ装置。

【請求項３】

無線網に収容された無線端末装置もしくは有線網に収容された有線端末装置のいずれかに設けられ、

前記無線端末装置と前記有線端末装置のとの間で秘匿性を保証する通信のために前記無線端末装置と前記有線端末装置との間に設定される第１のセキュリティアソシエーションに関する情報、乃至前記無線端末装置と前記有線端末装置との間で前記情報の認証を保証した通信を行うために前記無線端末装置と前記有線端末装置との間に設定される第２のセキュリティアソシエーションに関する情報を、前記無線端末装置と前記有線端末装置との間でトランスポート層以上の情報を用いた中継を行うゲートウェイ装置に提供するセキュリティ情報提供手段を
具備したことを特徴とする通信装置。

【請求項４】

前記第１乃至前記第２のセキュリティアソシエーションに関する情報は、前記無線端末装置と前記有線端末装置との間でトランスポート層以上の情報の通信を行う際に前記情報のセキュリティを管理するセキュリティサーバから前記ゲートウェイ装置に提供されることを特徴とする請求項３に記載の通信装置。

【請求項５】

無線網に収容された無線端末装置と有線網に収容された有線端末装置との間で秘匿性を保証する通信のために前記無線端末装置と前記有線端末装置との間に設定される第１のセキュリティアソシエーションに関する情報、乃至前記無線端末装置と前記有線端末装置との間で前記情報の認証を保証した通信を行うために前記無線端末装置と前記有線端末装置との間に設定される第２のセキュリティアソシエーションに関する情報を生成するセキュリティ情報生成手段と、

前記生成された第１乃至第２のセキュリティアソシエーションを前記無線端末装置乃至前記有線端末装置に配布するセキュリティ情報配布手段と
を具備したことを特徴とする制御装置。

【請求項６】

無線網に収容された無線端末装置と有線網に収容された有線端末装置との間でトランスポート層以上の情報の中継の制御を行う制御装置において、

前記無線端末装置と前記有線端末装置に設けられた検索鍵に対する、前記無線端末装置乃至前記有線端末装置に設けられた検索鍵に対して、前記無線端末装置と前記有線端末装置との間で秘匿性を保証する通信のために前記無線端末装置と前記有線端末装置との間に設定される第１のセキュリティアソシエーションに関する情報、乃至前記無線端末装置と前記有線端末装置との間で前記情報の認証を保証した通信を行うために前記無線端末装置と前記有線端末装置との間に設定される第２のセキュリティアソシエーションに関する情報を検索し抽出するセキュリティ情報検索手段を具備したことを特徴とする制御装置。

【請求項７】

無線網に収容された無線端末装置と有線網に収容された有線端末装置との間でトランスポート層以上の情報の中継を行う通信装置において、

前記情報の内容に基づいて前記無線端末装置と前記有線端末装置との間で中継処理を行う中継手段を動作させるか否かを選択し、

前記中継手段を動作させる場合には前記無線端末装置と前記有線端末装置との間で秘匿性を保証する通信のために前記無線端末装置と前記有線端末装置との間に設定される第１のセキュリティアソシエーションに関する情報、乃至前記無線端末装置と前記有線端末装置との間で前記情報の認証を保証した通信を行うために前記無線端末装置と前記有線端末装置との間に設定される第２のセキュリティアソシエーションに関する情報を用いて通信を行い、

前記中継手段を動作させない場合には前記無線端末装置と前記有線端末装置との間で通信を行うための第３のセキュリティアソシエーションに関する情報を設定し通信を行わせる選択手段を具備したことを特徴とする通信装置。

【請求項８】

無線網に収容された無線端末装置と有線網に収容された有線端末装置との間でゲートウェイ装置を介してトランスポート層以上の情報の中継を行う通信制御方法において、

第１のゲートウェイ装置を介して前記無線端末装置と前記有線端末装置との間で秘匿性を保証する通信のために前記無線端末装置と前記有線端末装置との間に設定される第１のセキュリティアソシエーションに関する情報、乃至前記第１のゲートウェイ装置を介して前記無線端末装置と前記有線端末装置との間で前記情報の認証を保証した通信を行うために前記無線端末装置と前記有線端末装置との間に設定される第２のセキュリティアソシエーションに関する情報を、第２のゲートウェイ装置に引き渡す工程と、

前記無線端末装置と前記有線端末装置との間の前記秘匿性乃至前記認証を保証した通信が、前記第１のゲートウェイ装置から前記第２のゲートウェイ装置に変化して経由された場合に、前記第１のゲートウェイ装置で行っていた前記トランスポート層以上の情報を利用した中継処理を前記引き渡された第１及び第２のセキュリティアソシエーションに関する情報を利用して前記第２のゲートウェイ装置において動作される工程と

を有することを特徴とする通信制御方法。

【請求項９】

無線網に収容された無線端末装置と有線網に収容された有線端末装置との間でゲートウェイ装置を介してトランスポート層以上の情報の中継を行う通信制御方法において、

第１のゲートウェイ装置を介して前記無線端末装置と前記有線端末装置との間で秘匿性を保証する通信のために前記無線端末装置と前記有線端末装置との間に設定される第１のセキュリティアソシエーションに関する情報、乃至前記第１のゲートウェイ装置を介して前記無線端末装置と前記有線端末装置との間で前記情報の認証を保証した通信を行うために前記無線端末装置と前記有線端末装置との間に設定される第２のセキュリティアソシエーションに関する情報を、第２のゲートウェイ装置に引き渡す工程と、

前記無線端末装置と前記有線端末装置との間の前記秘匿性乃至前記認証を保証した通信が、前記第１のゲートウェイ装置から前記第２のゲートウェイ装置に変化して経由された場合に、前記第１のゲートウェイ装置で行っていた前記トランスポート層以上の情報を利用した中継処理を前記引き渡された第１及び第２のセ

キュリティアソシエーションに関する情報及び前記トランスポート層以上の状態を利用して前記第２のゲートウェイ装置において動作される工程と
を有することを特徴とする通信制御方法。

【請求項１０】

無線網に収容された無線端末装置と有線網に収容された有線端末装置との間でトランスポート層以上の情報の中継を行うゲートウェイ装置において、

第１のゲートウェイ装置を通過した前記情報をカプセル化する第２のゲートウェイ装置と、

前記カプセル化された情報からカプセルを取り除き、前記カプセルが取り除かれた情報を前記トランスポート層以上の情報を利用して中継を行う必要があるか否かを判断し、必要な場合には中継を行う第３のゲートウェイ装置と、

前記第３のゲートウェイ装置から送られた情報をカプセル化するカプセル化手段と
を具備したことを特徴とするゲートウェイ装置。

【請求項１１】

ネットワークによって相互に通信可能な第１の通信装置と第２の通信装置との間で、トランスポート層以上の情報を利用した中継を行なうゲートウェイ装置において、

前記第１の通信装置と第２の通信装置との間で秘匿性を保証する通信のために、前記第１の通信装置と第２の通信装置との間に設定される第１のセキュリティアソシエーションに関する情報を保持する第１のセキュリティ情報保持手段と、

前記第１の通信装置と第２の通信装置との間で秘匿性を保証する通信を中継する際に前記第１のセキュリティアソシエーションに関する情報を利用して、前記第２の通信装置もしくは第２の通信装置に受信される暗号化された情報を復号化する情報復号化手段と、

前記復号化された情報に基づいて前記トランスポート層以上の情報を利用して中継処理を行う中継手段と、

前記中継手段が送信する情報を前記第１のセキュリティアソシエーションに関する情報を利用して秘匿化する情報暗号化手段と

を具備したことを特徴とするゲートウェイ装置。

【請求項１２】

ネットワークによって相互に通信可能な第１の通信装置と第２の通信装置との間で、トランスポート層以上の情報を利用した中継を行なうゲートウェイ装置において、

前記第１の通信装置と第２の通信装置との間で秘匿性を保証する通信のために、前記第１の通信装置と第２の通信装置との間に設定される第１のセキュリティアソシエーションに関する情報を保持する第１のセキュリティ情報保持手段と、

前記第１の通信装置と第２の通信装置との間で秘匿性を保証する通信を中継する際に前記第１のセキュリティアソシエーションに関する情報を利用して、前記第２の通信装置もしくは第２の通信装置に受信される暗号化された情報を復号化する情報復号化手段と、

前記復号化された情報に基づいて前記トランスポート層以上の情報を利用して中継処理を行う中継手段と、

前記中継手段が送信する情報を前記第１のセキュリティアソシエーションに関する情報を利用して秘匿化する情報暗号化手段と

を具備したことを特徴とするゲートウェイ装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、トランスポート層を利用する通信に介在する中継装置、通信装置、制御装置および通信制御方法に関する。

【０００２】

【従来の技術】

近年無線によって音声信号のみならず、データ通信も行う要求が高まっている。ＴＣＰ（Transmission Control Protocol）は、有線データ通信において信頼性のあるトランスポート層プロトコルとして広く使われているが、このプロトコルをそのまま無線に適用すると以下のような問題が発生する。

【０００３】

有線通信におけるＴＣＰパケット損失はネットワークの輻輳を意味するため、ＴＣＰはパケット損失を検出するとデータの送出レートを下げて輻輳を回避するように設計されている。パケット損失は、同一シーケンス番号を持つACKが指定された数（通常はオリジナルに加えて３個）以上受信された場合、およびRTTとその偏差から定められるタイマがタイムアウトした場合に検出される。

【０００４】

このため無線区間のエラーおよびハンドオフによるＴＣＰパケット損失、乃至はリンク層でのエラー回復に時間がかかった場合も輻輳と解釈されるので、必要以上に輻輳回避を行う結果、スループットが利用できる無線帯域以下に低下する場合が多くなる。また、無線区間のエラーをエンド・エンドでTCPによって再送すると、有線部分の帯域が無駄であるし時間もかかる。また、リンク層がエラー回復をしている場合は同じデータを重複して送ることになる。

【０００５】

このような問題を解決するために、有線側端末と無線側端末の間に（多くの場合は無線と有線の境界部分に）、TCPの性能を向上させるためのプロキシー（PEP：Performance Enhancement Proxy）を挿入する方法が提案されている。

【０００６】

Split Connectionによる方法は、TCPコネクションをProxy（以下ではTCP-GWと呼ぶ）に於いて、有線側TCPコネクションと無線側TCPコネクションとに分割する方法である。有線端末から無線端末にデータを送信する場合を想定する。

【０００７】

TCP-GWは無線端末の代わりに有線端末にACKを返すので、無線のエラーの影響（パケット損失乃至大きな遅延変動）は、有線端末から隠蔽される。TCPデータパケットが失われた場合には、TCP-GWが有線端末の代わりにデータの再送を行う。無線側のTCPは無線用にチューニングしたものであっても良い。例えば、無線側TCPはselective ACKオプション（IETF RFC2018）を使って、高いパケット損失率でも性能が大きく劣化しないようにしたものであっても良い。また、輻輳制御のアルゴリズムを変更して、TCPパケット損失があっても、帯域を絞り過ぎない用にしたものであってもよい。

【０００８】

Snoop proxyによる方法は、TCP-GWがTCPコネクションを終端とみなしてしまうので、TCPのエンド・エンドセマンティクス（TCPのACKが送信端末に戻って来た場合には、そのACKのシーケンス番号までは受信端末に到達している）を破るという問題に対応するものである。Snoop proxyは、TCPデータパケットをバッファするが、その時点では送信端末にACKは返さない。本来の受信端末からのACKが帰って来た時点でACKを送信端末に中継し、バッファしていたTCPデータパケットを廃棄する。但し、ACKが重複ACKであり、本来の送信端末からの再送をトリガするものである場合、重複ACKは廃棄して、Snoop proxyがTCPデータパケットの再送を行う。また、Snoop proxyはタイムアウト再送も行う。このようにして、無線エラーの影響の大部分を、送信端末から隠蔽する。

【０００９】

一方で、このような無線データ通信は、近隣の誰もが無線信号を傍受可能であり、かつ移動環境で使用する場合が多いため、セキュリティに対する要求も高くなる。

【００１０】

インターネットにおけるセキュリティ確保の一方法として、IPSecによるものがある（IETF RFC2401，2402，および2408など）。セキュリティは様々なレイヤで提供されるが、IPSecはIP層でセキュリティを確保するための方式である。IPSecでは、（１）IPヘッダの経路上で変更されない部分と、（２）IPペイロードに対してデータが経路上で改竄されていないことと、（３）そのデータが本来の送信者によって生成されたこと、を保証する機能がある。このためには、AH（Authentication Header）を、IPヘッダとIPペイロードとの間に挿入しなければならない。また、IPペイロードに対して、秘匿性、改竄のないこと、および送信者による生成を保証する機能もある。このためには、ESP（Encapsulating Security Payload）を用いる。なお、AHとESPを組み合わせて使うこともできる。

【００１１】

また、IPSecやMobileIPでは、IPSecやMobileIPの機能を持つゲートウェイ装置やエージェント装置で、本来のパケットを別のパケットに包んで（カプセル化）

して、ゲートウェイ装置やエージェント装置、乃至は本来のパケットの目的地である端末まで送信する技術が利用される。本来のパケットがカプセル化された状態で辿る経路をトンネルと表現する。

【００１２】

【発明が解決しようとする課題】

以上説明したように、無線網に収容された無線端末装置と有線網に収容された有線端末装置との間で通信を行う際に、TCP-GW乃至Snoop proxyのようなTCPの性能を向上させるための装置とIPSecのようなセキュリティを提供する方法とは、共に無線データ通信環境での要求が高いが、このような装置と方法とを組み合わせて使用する場合には以下に説明するような問題があった。

【００１３】

つまり、TCPヘッダはIPSecによって保護されているIPペイロードに含まれるが、TCPの性能を向上させるProxyは、TCPヘッダに含まれる情報を知り、かつ場合によって変更しなければならないことが問題である。また、送信されるデータに改竄のないことを保証すると、TCP-GWが本来の受信端末に代わってACKを送信することはできなくなる。これはTCP-GW自信がACK情報を生成する必要が生じてくるためである。更に送信されるデータに秘匿性を要求すると、TCP-GW乃至Snoop ProxyはTCPヘッダの情報が読み取れないので、有効な動作が不可能になる。

【００１４】

また、IPSecやMobileIPなどで利用される「トンネル」の途中にProxy装置がある場合、このproxy装置は有効に機能しない。なぜなら、例えばTCP-GWがカプセル化されたパケットを処理するべきか否かのフィルタにかけるために、カプセル化しているパケットのヘッダを調べても、そのヘッダはペイロードがTCPパケット

であることを表示していないからである。

【００１５】

そこで、本発明は上記従来の問題点に鑑みてなされたもので、TCP-GWやSnoopに代表されるProxy装置と、IPSecに代表されるセキュリティプロトコルとを組み合わせることによって、セキュリティを維持しつつ無線端末装置と有線端末装置

とのデータ通信を効率よく行い、またIPSecやMobileIPなどで利用される「トンネル」を通るカプセル化されたパケットに対しても有効に機能するゲートウェイ装置、通信装置、制御装置、および通信制御方法の提供を目的とする。

【００１６】

【課題を解決するための手段】

以上に述べた課題を解決するため、本発明におけるゲートウェイ装置は、無線網に収容された無線端末装置と有線網に収容された有線端末装置との間でトランスポート層以上の情報の中継を行うゲートウェイ装置において、前記無線端末装置と前記有線端末装置との間で秘匿性を保証する通信のために、前記無線端末装置と前記有線端末装置との間に設定される第１のセキュリティアソシエーションに関する情報を保持する第１のセキュリティ情報保持手段と、前記無線端末装置と前記有線端末装置との間で秘匿性を保証する通信を中継する際に前記第１セキュリティアソシエーションに関する情報を利用して前記無線端末装置もしくは前記有線端末装置に受信される暗号化された情報を復号化する情報復号化手段と、前記復号化された情報に基づいて前記トランスポート層以上の情報を利用して中継処理を行う中継手段と、前記中継手段が送信する情報を前記第１のセキュリティアソシエーションに関する情報を利用して秘匿化する情報暗号化手段とから構成される。

【００１７】

また、本発明におけるゲートウェイ装置は、無線網に収容された無線端末装置と有線網に収容された有線端末装置との間でトランスポート層以上の情報の中継を行うゲートウェイ装置において、前記無線端末装置と前記有線端末装置との間で情報の認証を保証した通信を行うために、前記無線端末装置と前記有線端末装置との間に設定される第１のセキュリティアソシエーションに関する情報を保持する第１のセキュリティ情報保持手段と、前記無線端末装置と前記有線端末装置との間で前記認証を保証された情報を前記トランスポート層以上の情報を利用して中継処理を行う中継手段と、前記中継手段が中継する前記認証が保証された情報および前記中継手段が必要に応じて新たに生成した情報に対して前記第１のセキュリティアソシエーションに関する情報を利用して、前記認証が保証された情

報を保証する認証情報を付加する認証情報手段とから構成される。

【００１８】

また、本発明の通信装置は、無線網に収容された無線端末装置もしくは有線網に収容された有線端末装置のいずれかに設けられ、前記無線端末装置と前記有線端末装置のとの間で秘匿性を保証する通信のために前記無線端末装置と前記有線端末装置との間に設定される第１のセキュリティアソシエーションに関する情報、乃至前記無線端末装置と前記有線端末装置との間で前記情報の認証を保証した通信を行うために前記無線端末装置と前記有線端末装置との間に設定される第２のセキュリティアソシエーションに関する情報を、前記無線端末装置と前記有線端末装置との間でトランスポート層以上の情報を用いた中継を行うゲートウェイ装置に提供するセキュリティ情報提供手段とから構成される。

【００１９】

また、本発明における制御装置は、無線網に収容された無線端末装置と有線網に収容された有線端末装置との間で秘匿性を保証する通信のために前記無線端末装置と前記有線端末装置との間に設定される第１のセキュリティアソシエーションに関する情報、乃至前記無線端末装置と前記有線端末装置との間で前記情報の認証を保証した通信を行うために前記無線端末装置と前記有線端末装置との間に設定される第２のセキュリティアソシエーションに関する情報を生成するセキュリティ情報生成手段と、前記生成された第１乃至第２のセキュリティアソシエーションを前記無線端末装置乃至前記有線端末装置に配布するセキュリティ情報配布手段とから構成される。

【００２０】

また、本発明の制御装置は、無線網に収容された無線端末装置と有線網に収容された有線端末装置との間でトランスポート層以上の情報の中継の制御を行う制御装置において、前記無線端末装置と前記有線端末装置に設けられた検索鍵に対する、前記無線端末装置乃至前記有線端末装置に設けられた検索鍵に対して、前記無線端末装置と前記有線端末装置との間で秘匿性を保証する通信のために前記無線端末装置と前記有線端末装置との間に設定される第１のセキュリティアソシエーションに関する情報、乃至前記無線端末装置と前記有線端末装置との間で前

記情報の認証を保証した通信を行うために前記無線端末装置と前記有線端末装置との間に設定される第２のセキュリティアソシエーションに関する情報を検索し抽出するセキュリティ情報検索手段とから構成される。

【００２１】

また、本発明における通信装置は、無線網に収容された無線端末装置と有線網に収容された有線端末装置との間でトランスポート層以上の情報の中継を行う通信装置において、前記情報の内容に基づいて前記無線端末装置と前記有線端末装置との間で中継処理を行う中継手段を動作させるか否かを選択し、前記中継手段を動作させる場合には前記無線端末装置と前記有線端末装置との間で秘匿性を保証する通信のために前記無線端末装置と前記有線端末装置との間に設定される第１のセキュリティアソシエーションに関する情報、乃至前記無線端末装置と前記有線端末装置との間で前記情報の認証を保証した通信を行うために前記無線端末装置と前記有線端末装置との間に設定される第２のセキュリティアソシエーションに関する情報を用いて通信を行い、前記中継手段を動作させない場合には前記無線端末装置と前記有線端末装置との間で通信を行うための第３のセキュリティアソシエーションに関する情報を設定し通信を行わせる選択手段とから構成される。

【００２２】

また、本発明の通信制御方法は、無線網に収容された無線端末装置と有線網に収容された有線端末装置との間でゲートウェイ装置を介してトランスポート層以上の情報の中継を行う通信制御方法において、第１のゲートウェイ装置を介して前記無線端末装置と前記有線端末装置との間で秘匿性を保証する通信のために前記無線端末装置と前記有線端末装置との間に設定される第１のセキュリティアソシエーションに関する情報、乃至前記第１のゲートウェイ装置を介して前記無線端末装置と前記有線端末装置との間で前記情報の認証を保証した通信を行うために前記無線端末装置と前記有線端末装置との間に設定される第２のセキュリティアソシエーションに関する情報を、第２のゲートウェイ装置に引き渡す工程と、前記無線端末装置と前記有線端末装置との間の前記秘匿性乃至前記認証を保証した通信が、前記第１のゲートウェイ装置から前記第２のゲートウェイ装置に変化

して経由された場合に、前記第１のゲートウェイ装置で行っていた前記トランスポート層以上の情報を利用した中継処理を前記引き渡された第１及び第２のセキュリティアソシエーションに関する情報を利用して前記第２のゲートウェイ装置において動作される工程とを有する。

【００２３】

また、本発明における通信制御方法は、無線網に収容された無線端末装置と有線網に収容された有線端末装置との間でゲートウェイ装置を介してトランスポート層以上の情報の中継を行う通信制御方法において、第１のゲートウェイ装置を介して前記無線端末装置と前記有線端末装置との間で秘匿性を保証する通信のために前記無線端末装置と前記有線端末装置との間に設定される第１のセキュリティアソシエーションに関する情報、乃至前記第１のゲートウェイ装置を介して前記無線端末装置と前記有線端末装置との間で前記情報の認証を保証した通信を行うために前記無線端末装置と前記有線端末装置との間に設定される第２のセキュリティアソシエーションに関する情報を、第２のゲートウェイ装置に引き渡す工程と、前記無線端末装置と前記有線端末装置との間の前記秘匿性乃至前記認証を保証した通信が、前記第１のゲートウェイ装置から前記第２のゲートウェイ装置に変化して経由された場合に、前記第１のゲートウェイ装置で行っていた前記トランスポート層以上の情報を利用した中継処理を前記引き渡された第１及び第２のセキュリティアソシエーションに関する情報及び前記トランスポート層以上の状態を利用して前記第２のゲートウェイ装置において動作される工程とを有する。

【００２４】

また、本発明のおけるゲートウェイ装置は、無線網に収容された無線端末装置と有線網に収容された有線端末装置との間でトランスポート層以上の情報の中継を行うゲートウェイ装置において、第１のゲートウェイ装置を通過した前記情報をカプセル化する第２のゲートウェイ装置と、前記カプセル化された情報からカプセルを取り除き、前記カプセルが取り除かれた情報を前記トランスポート層以上の情報を利用して中継を行う必要があるか否かを判断し、必要な場合には中継を行う第３のゲートウェイ装置と、前記第３のゲートウェイ装置から送られた情

報をカプセル化するカプセル化手段とから構成される。

【００２５】

また、本発明のおけるゲートウェイ装置は、ネットワークによって相互に通信可能な第１の通信装置と第２の通信装置との間で、トランスポート層以上の情報を利用した中継を行なうゲートウェイ装置において、前記第１の通信装置と第２の通信装置との間で秘匿性を保証する通信のために、前記第１の通信装置と第２の通信装置との間に設定される第１のセキュリティアソシエーションに関する情報を保持する第１のセキュリティ情報保持手段と、前記第１の通信装置と第２の通信装置との間で秘匿性を保証する通信を中継する際に前記第１のセキュリティアソシエーションに関する情報を利用して、前記第２の通信装置もしくは第２の通信装置に受信される暗号化された情報を復号化する情報復号化手段と、前記復号化された情報に基づいて前記トランスポート層以上の情報を利用して中継処理を行う中継手段と、前記中継手段が送信する情報を前記第１のセキュリティアソシエーションに関する情報を利用して秘匿化（暗号化）する情報暗号化手段とから構成される。

【００２６】

また、本発明のおけるゲートウェイ装置は、ネットワークによって相互に通信可能な第１の通信装置と第２の通信装置との間で、トランスポート層以上の情報を利用した中継を行なうゲートウェイ装置において、前記第１の通信装置と第２の通信装置との間で秘匿性を保証する通信のために、前記第１の通信装置と第２の通信装置との間に設定される第１のセキュリティアソシエーションに関する情報を保持する第１のセキュリティ情報保持手段と、前記第１の通信装置と第２の通信装置との間で秘匿性を保証する通信を中継する際に前記第１のセキュリティアソシエーションに関する情報を利用して、前記第２の通信装置もしくは第２の通信装置に受信される暗号化された情報を復号化する情報復号化手段と、前記復号化された情報に基づいて前記トランスポート層以上の情報を利用して中継処理を行う中継手段と、前記中継手段が送信する情報を前記第１のセキュリティアソシエーションに関する情報を利用して秘匿化する情報暗号化手段とから構成される。

【００２７】

なお、無線通信端末および有線通信端末は、それら装置と情報の送受信もしくは中継がなされるサーバを含んだものであっても良い。また、通信装置は無線通信端末、有線通信端末乃至ルータであっても良い。

【００２８】

【発明の実施の形態】

以下、本発明の実施の形態について図面を参照して説明する。

【００２９】

図１は本発明のネットワーク構成図であり、ルータ７０１を挟んで、ネットワーク２０１側とネットワーク２０２側とに分けられる。これらの間でネットワーク運営の主体が異なっていても構わない。ネットワーク２０１は有線網に有用されたTCP/IP端末１０１～１０３（有線端末装置）を収容し、IPパケットを交換するルータ７０１によってネットワーク２０２と相互接続されている。ここで、ネットワーク２０１と類似のネットワークが複数ネットワーク２０２に接続されていても良い。また、ネットワーク２０１がネットワーク２０２以外のネットワークと相互接続されていても良い。ネットワーク２０２側は移動をサポートしているものとする。但し、移動の有無は特許の本質とは無関係である。移動はMobile IPのようなIP層による実現、セルラー網のようなリンク層による実現などがあるが、その方法も問わない。移動を実現するために必要な要素は図示していない。ネットワーク２０２はTCP-GW４０１と４０２とによってネットワーク２０３と２０４とを、TCP-GW４０３によって基地局３０５と３０６とを、それぞれ収容する。

【００３０】

TCP-GWはSnoop ProxyのようなTCPを意識したリンク層再送機能を持つノードであっても良いし、更に一般的なプロキシー装置であっても構わないが、以下ではTCP-GWで代表する。更にネットワーク２０２はセキュリティサーバ６０１を持つ。ネットワーク２０３と２０４は、それぞれ基地局３０１と３０２、基地局３０３と３０４を収容する。基地局３０１のエリアには無線網に収容された移動端末５０１と５０２、基地局３０２のエリアには無線網に収容された移動端末５０３

、基地局３０４のエリアには無線網に収容された移動端末５０４と５０５、基地局３０５のエリアには無線網に収容された移動端末５０６、そして基地局３０６のエリアには無線網に収容された移動端末５０７と５０８が存在する状態を示している。移動端末５０１～５０８（無線端末装置）はTCP/IP端末である。

【００３１】

このような状況下で、例えば端末１０１と移動端末５０１の間でIPSecを利用してセキュリティを保証したTCP/IP通信を行う場合を想定する。IPSecによる通信を行うためには、端末１０１と移動端末５０１との間にIPSec SA（Security Association、以下SAと記す）が確立されている必要がある。

【００３２】

SAは一方向の関係を示すので、双方向の関係には２つのSAが必要となる。１つのSAに適用されるセキュリティプロトコルは１つに制限される。但し、必要なら２点の間で複数のSAを設定しても良い。SAを識別する情報は、（１）SPI（Security Parameter Index）、（２）IP destination address、（３）Security protocol identifierの３つである。SPIはローカルで一意なビット列である。SPIは、AHおよびESPヘッダに含まれ、受信側が受信パケットを処理するために必要なSAを決定するために使われる。IP destination addressはSAの終点を示す。SAの終点はエンドユーザシステムであっても、ファイアウォールのようなものであっても良い。Security protocol identifierは、SAがAH乃至ESPを使うか否かを示す。

【００３３】

セキュリティアソシエーションデータベース（SAD）には、以下のような情報が含まれる。

【００３４】

・シーケンス番号カウンタ：AH乃至ESPヘッダのシーケンス番号フィールドを生成するために使用される。

【００３５】

・シーケンス番号カウンタオーバフロー:オーバフローした場合は、それ以上のパケット送信は禁止される。

【００３６】

・Anti-reply ウィンドウ:AHまたはESPパケットが第３者による再送でないことを保証するために、そのシーケンス番号は、ここで指定されるスライディングウィンドウの範囲になければならない。

【００３７】

・AH情報:認証アルゴリズム、鍵、鍵の生存時間、およびAHに関連するパラメータ。

【００３８】

・ESP情報:暗号化と認証アルゴリズム、鍵、初期化の値、鍵の生存時間、およびESPに関連するパラメータ。

【００３９】

・SAの生存時間:このSAが新たなSAで置き換えられなければならない、時間インターバル、乃至はバイト数。およびこのような置き換えを行わなければならないか否かの指定。

【００４０】

・IPSecプロトコルモード:トンネル、トランスポート乃至ワイルドカードモード。

【００４１】

・Path MTU:観測されたパスの最大transmission unit（IPフラグメントなしでそのパス経由で伝送できる最大サイズ）。およびその情報の新しさ。

【００４２】

ユーザのポリシーによって、IPSecをいかにIPトラフィックに適用するかを決めることができる。つまりIPSecを適用するか否か、適用するとすればどのSAを利用するかを選択できる。このような情報はセキュリティポリシーデータベース（SPD）に含まれている。

【００４３】

SPDのエントリは、以下のselectorによって定められる。

【００４４】

・Destination IP address:範囲を示すものであっても良い。

【００４５】

・Source IP address:範囲を示すものであっても良い。

【００４６】

・User ID:システムのユーザ識別子。

【００４７】

・Data sensitivity level:秘密乃至そうでないかなど。

【００４８】

・トランスポート層プロトコル:UDP,TCPなどを指定するプロトコル番号。

【００４９】

・IPSec プロトコル:AH、ESP乃至AH/ESP。

【００５０】

・Source and destination ports:TCP乃至UDPのポート番号。

【００５１】

・IPv6 class, IPv6 flow label

・IPv4 Type of Service (TOS)

このように識別されるSPDの各エントリには、１つ以上のSAが対応している。

【００５２】

SAは手動で設定しても良いが、Internet Key Exchange (IKE) によって自動的に設定することも可能である。IKEは２つのフェーズに分けられる。フェーズ１では、IKE SAを確立しその後の通信の安全を図る。フェーズ２では、IKE SAの下で、AH乃至はESPのためのSAのパラメータを交換する。

【００５３】

さて、TCP-GWに代表されるプロキシーが機能するためには、TCP-GWがSAの少なくとも一部の情報を知っている必要がある。この情報とはより具体的には、暗号化を解いて必要な処理後に再び暗号を掛けるために必要な情報であり、また、プロキシーがパケットを生成する場合にそのパケットを正しく認証された形式にするために必要な情報である。

【００５４】

このようなプロキシーを機能させるための方法として、以下の方式が考えられ

る。

【００５５】

（方式１）各種情報を手動で設定する。

【００５６】

（方式２）IKEのフェーズ２で交換されるSA情報から得る。つまり、IKE SAの情報を知っていてIPSec SA情報を傍受したエンティティがプロキシーに情報を与える。

【００５７】

（方式３）SAのいずれかの端点から提供を受ける。

【００５８】

（方式４）プロキシー自ら、乃至セキュリティサーバがSA情報を生成し、各端点と必要ならプロキシーに提供する。

【００５９】

以下では、方式３と方式４について詳しく述べる。

【００６０】

最初に（方式３）について述べる。端末１０１と移動端末５０１の間で、IKE SAが確立されているとする。これから行おうとする通信に適用するべきIPSec SAは、確立されている場合と確立されていない場合とがある。IPSec SA確立されていない場合は、端末１０１のセキュリティ情報管理１１２４（図３参照、セキュリティ情報提供手段（請求項３））と移動端末５０１のセキュリティ情報管理１５２４（図４参照、セキュリティ情報提供手段（請求項３））の間で、IKEのフェーズ２の手順でIPSec SAを確立すれば良い。セキュリティ情報管理１１２４（選択手段（請求項７））、１５２４は、自らの持つSADとSPDに、このIPSec SA確立で発生した関連する情報を記憶する。なお、IPSec SAとして、プロキシーの介在を許容するものと、許容しないものを設けても良い。更に、プロキシーに暗号を解くことは許すが、新たなパケットの生成乃至パケット内容の変更は許容しないクラスがあっても良い。これはSPDのselectorのdata sensitivity levelに、その識別を行う分類を設けるのが自然であるが、例えばポート番号で識別しても良い。

【００６１】

以下では、プロキシーの介在を許容するIPSec SAを主に扱う。プロキシーの介在を許容しないIPSec SAについては、従来のIPSecと同様に動作する。

【００６２】

さて、端末１０１と移動端末５０１は、セキュリティサーバ６０１（セキュリティ情報生成手段（請求項５）、セキュリティ情報配布手段（請求項５）、制御装置（請求項６））およびTCP-GW４０１～４０３を信頼できる装置として扱う。例えば、それらがある信頼できるネットワーク運営主体によって信頼できる装置として運用されている場合が想定できる。このネットワークのTCP-GWに代表されるプロキシー機能を利用するためには、セキュリティサーバ６０１にIPSec SA情報を提供する必要があることは、端末１０１乃至移動端末５０１の少なくともいずれか一方には認識されていることを仮定している。なお、セキュリティサーバ６０１でなく、TCP-GW４０１に直接IPSec SA情報を提供してもTCP-GWとして有効に動作できるが、利用する個別のプロキシーを端末１０１乃至移動端末５０１が認識しなければならない。TCP-GWやSnoopなどは、本来その存在が端末から見えないので、これはあまり良い方法ではない。また、端末１０１、移動端末５０１のいずれが提供しても良いが、無線対応のプロキシーを利用すべきであることをより容易に把握できる移動端末５０１が提供すると仮定する。まず、これから送信するIPSec SA情報を保護するために、移動端末５０１とセキュリティサーバ６０１の間に何らかのセキュリティアソシエーションが必要である。セキュリティアソシエーションは、IPSecを使うと仮定する。移動端末５０１とセキュリティサーバ６０１の間で、最初にIKE SAを確立し、次にAHとESPの両方を用いるIPSec SAを確立する。このIPSec SAを用いて、移動端末５０１のセキュリティ情報管理１５２４から、セキュリティサーバ６０１のセキュリティ情報管理１６２４（図５参照、セキュリティ情報生成手段（請求項５）、セキュリティ情報配布手段（請求項５）、セキュリティ情報検索手段（請求項６））に向けて、端末１０１と移動端末５０１の間のプロキシー介在を許容するIPSec SA情報を送信する。セキュリティ情報管理１６２４は、この情報をSPDとSADに記憶する。

【００６３】

図２はTCP-GWのブロック構成図であり、上述したSnoop Proxyのようなものであっても良くその場合の構成は異なる。また図３は端末１０１のブロック構成図であり、図４は移動端末５０１のブロック構成図であり、図５はセキュリティサーバ６０１のブロック構成図である。なお、図中の実線矢印はデータの流れ、破線矢印は制御の流れを示す。

【００６４】

以下で、TCP-GW４０１は、端末１０１と移動端末５０１の間のトラフィックを検出したことを契機に、IPSec SA情報をセキュリティサーバ６０１から取得する。ここでは、IKE SAによって、上記のプロキシー介在を許容するIPSec SAを確立するためのトラフィックを検出したとする。IKEはUDPのポート番号500を利用しているので、IP入力部１４２３でIPヘッダを見ていれば、この通信の存在がわかる。端末１０１と移動端末５０１の間の他の種類の通信であっても構わない。これらの存在は、端末１０１と移動端末５０１の間で、今後も何らかの通信が行われる可能性が高いことを示している。従って、TCP-GW４０１のセキュリティ情報管理１４２４（第１のセキュリティ情報保持手段（請求項１，２））が、セキュリティサーバ６０１のセキュリティ情報管理１６２４に対して、端末１０１と移動端末５０１の間のIPSec SAに関する情報を提供するように要求する。例えば端末１０１と移動端末５０１のＩＰアドレスの組を検索鍵として予めセキュリティサーバ６０１に記憶しておくことも一手法である。

【００６５】

セキュリティサーバ６０１のセキュリティ情報管理１６２４は、TCP-GW４０１のセキュリティ情報管理１４２４からの要求を受けた時点では、まだ端末１０１と移動端末５０１の間のIPSec SAを持っていないかも知れない。なぜなら、この要求はIPSec SAを設定するためのトラフィックを検出して行われたものだからである。セキュリティ情報管理１６２４は、そのような要求があったことをタイムアウトするまで記憶しておいて、要求にあうIPSec SA情報を得る度に、TCP-GW４０１のセキュリティ情報管理１４２４に、IPSec SA情報を提供する。

【００６６】

このようにして、TCP-GW４０１のセキュリティ情報管理１４２４が、セキュリ

ティサーバ６０１のセキュリティ情報管理１６２４から、端末１０１と移動端末５０１の間のIPSec SAに関する情報を得ると、これをセキュリティ情報管理１４２４のSPDとSADに記憶する。更に、IP入力部１４２３でフィルタを設定して、端末１０１と移動端末５０１の間のプロキシー介在を許容するIPSec SAによるパケットでかつTCPの通信であるという条件にマッチする時には、TCP層まで上げるようにする。なお、IPSec SA情報要求がタイムアウトする時点で、更に端末１０１と移動端末５０１の間での通信がTCP-GW４０１を通過すると見込まれる場合には、要求を更新する。

【００６７】

次に、プロキシーを許容するIPSec SAを利用して、端末１０１のPEP利用アプリケーション１１６２（図３参照）と移動端末５０１のPEP利用アプリケーション１５６２（図４参照）が通信を行う。なお、アプリケーションでプロキシーを許容するか否かを分けているのは便宜的なもので、実際にはTCPのコネクション毎に使い分けが可能である。PEP利用アプリケーション１１６２がPEP利用アプリケーション１５６２に対して、TCPのコネクション設定を行うとする。PEP利用アプリケーション１１６２は、例えばUNIXのsocketインタフェースによって、OSに対してTCPコネクション設定を要求できる。この際、例えばsocketのオプションによって、このTCPコネクションをプロキシー介在を許容するか否かを指定できる。既に述べたように、ここではプロキシー介在を許容する。これは、例えばSPDエントリのData sensitivity level selectorの値として設定される。他のselectorの値は、destination IP addressとして移動端末５０１のIPアドレス、source IP addressとして端末１０１のIPアドレス、UserIDとしてPEP利用アプリケーション１１６２のユーザ識別子、Transport layer protocolとしてTCP、IPSec protocolとして例えばAH/ESP（他にAHあるいはESPが可能）、source/destination portとして適当なポート番号などとなる。IP出力部１１２２を監視しているセキュリティ情報管理１１２４は、出力IPパケット毎にSDPエントリを検索し、対応するIPSec SAを見付ける。Selectorが上記の値を持つパケットに対しては、既に述べたプロキシー介在を許容するIPSec SAが対応する。するとセキュリティ情報管理１１２４は、IPSec SAに指定されたアルゴリズムと鍵などによって、パケ

ットを暗号化し認証のための情報を付加するように、暗号機能１１２６と認証機能１１２５を制御する。トランスポートモードとトンネルモードのうち、ここでは前者を利用するので、図６（a）のパケットを処理後のパケットは図６（ｂ）に示すフォーマットになる。ここで、一般に暗号化後にはTCPヘッダとデータの境界は保存されない。また、AH認証対象は、IPヘッダの経路上での変化による結果を予測できない部分（例えばTTLなど）は含まない。

【００６８】

このように処理されたパケットは、有線IF出力部１１４２によってネットワーク２０１に送信され、更にルータ７０１、ネットワーク２０２を経由して、TCP-GW４０１に到着する。有線側IF入力部１４４６を経てIP入力部１４２３に到着したパケットは、SPI （Security Parameter Index）、IP destinationaddress、Security protocol identifierの3つによって識別されるIPSec SAの指定に従って処理される。識別するパラメータの値は、セキュリティサーバ６０１から提供されたものであり、セキュリティ情報管理１４２４によってIP入力部に設定されている。セキュリティ情報管理１４２４が認証機能１４２５（認証情報手段（請求項２））と暗号機能１４２６（情報復号化手段（請求項１）、情報暗号化手段（請求項１））を制御して、図６（ｂ）に示すIPSecパケットを、図６（a）に示す元のパケットの形に戻す。

【００６９】

元のパケットの情報からTCP中継処理を行うか否かをIP入力部１４２３が判断し、中継処理を行うものとしてTCP入力部１４０５に渡す。最も単純な判断基準はTCPなら全てTCP接続を利用して中継するというものであるが、他の属性も使用してTCPだがTCP情報を利用した中継をしないようにしても良い（IP中継となる）。このパケットは、その内容に応じて、TCP中継部１４０２（中継手段（請求項１，２））の有線→無線１４０７、TCP入力部１４０５および無線TCP出力部１４０８で処理される。例えば、SYNパケットなら、新たなTCPコネクションが設定されるものとして対応する状態を生成する。必要なら適当なオプションを追加するなどして、無線TCP出力部１４０８に中継する。更に、TCP出力部１４０４からSYN/ACKを返す（Snoopの場合は返さない）。別の例として、データパケットなら、

後で再送する可能性があるので、バッファにコピーを蓄積してから、無線TCP出力部１４０８に渡す。更に、TCP出力部１４０４からそのデータパケットに対するACKを返す（Snoopの場合は返さない）。なお、ここで扱っているパケットは、TCP-GW４０１が生成したものを含め、全て端末１０１と移動端末５０１の間で送受信されているかのように、IPヘッダのアドレスフィールドが設定されている。つまり、TCPゲート４０１存在は隠されている。

【００７０】

無線TCP出力部１４０８およびTCP出力部１４０４は、パケットをIP出力部１４２２に渡す。セキュリティ情報管理１４２４は、パケットの情報からSPDのエントリを識別するselector情報を得て、SPDを検索して対応するIPSec SAを得る。このIPSec SAに関する情報をSADから取得して、それに応じて暗号機能１４２６と認証機能１４２５を制御して、再びパケットを図６（ｂ）に示すIPSecパケットの形にする。ここで同じパケットであっても、TCP-GWに受信されたIPSecパケットと、TCP-GWから送信されるIPSecパケットの内容は一般に異なる。例えば、TCP-GW４０１は、ACKを中継するのではなく生成するので訂正のために付与されるIPSecのAHないしESPのシーケンス番号は一般に異なる。これらのパケットは、無線側IF出力部１４４３からネットワーク２０３へ、有線側IF出力部１４４５からネットワーク２０２へ、それぞれ送信される。

【００７１】

なお、Snoopの場合は、Snoop proxyに受信されたIPSecパケットと、Snoop proxyから送信されるIPSecパケットの内容は多くの場合同じにできる。

【００７２】

Snoopは重複ACKを中継せずに捨てることがあるが、これはIPネットワーク内で自然に失われるのと同じであり、IPSec的に特に問題無い。Snoopが本来のTCP送信ホストの代わりに再送を行うことがあるが、これはオリジナルのコピーを再送すれば良いが、IPSecのAnti-replyによって受信端末で捨てられる可能性がある。これを防ぐためには、認証のためのシーケンス番号が、Anti-replyウィンドウの範囲内に収まっている必要がある。これらの条件が満たされれば、Snoopの場合には、IPSecパケットから元のTCP/IPヘッダ情報を取り出せれば良いのであっ

て、一度オリジナルの形に戻したパケットを再びIPSecパケットに変更する必要は無い。従って、Snoop proxyに認証を掛けるために鍵情報を与えなければ、端末１０１と移動端末５０１の間で、情報の改竄がなかったことと、本来の送信者から送信されたパケットであることはIPSec的に保証できる。Snoop proxyに暗号を解くためのSA情報を持てば機能できる。

【００７３】

ネットワーク２０３へ送信されたパケットに注目すると、これは基地局３０１経由で移動端末５０１によって受信される。無線IF入力部１５４３を経てIP入力部１５２３に到着したパケットは、SPI（Security Parameter Index）、IP destination address、Security protocol identifierの３つによって識別されるIPSec SAの指定に従って処理される。セキュリティ情報管理１５２４が認証機能１５２５と暗号機能１５２６を制御して、図６（ｂ）に示すIPSecパケットを、図６（a）に示す元のパケットの形に戻す。そして、パケットに載っていた情報は、PEP利用アプリケーション１５６２に渡される。

【００７４】

次に（方式４）、つまりセキュリティサーバ６０１がIPSec SA情報を生成し、端末１０１と移動端末５０１、およびTCP-GW４０１に生成したIPSec SA情報を渡す場合について述べる。

【００７５】

移動端末５０１のセキュリティ情報管理１１２４が、セキュリティサーバ６０１のセキュリティ情報管理１６２４に対し、端末１０１との間のプロキシーの介在を許容するIPSec SA情報を生成するように依頼する。依頼にはIPSecなどでセキュリティの確保された通信路を用いる。セキュリティ情報管理１６２４は、依頼に応じたIPSec SA情報を生成すると、これをセキュリティの確保された通信路で、移動端末５０１、端末１０１、およびTCP-GW４０１に提供する。移動端末５０１には、依頼の応答として提供すれば良い。端末１０１に対しては、セキュリティサーバ６０１から直接提供しても良いし、移動端末５０１から提供しても良い。TCP-GWに対しては、例えば移動端末５０１の位置情報から、TCP-GW４０１がIPSec SAを利用する可能性の高いと判断できれば、セキュリティサーバ６０１が

自発的に送信すれば良い。さもなければTCP-GW４０１が、端末１０１と移動端末５０１の間の通信を検出してから、セキュリティサーバ６０１に要求することになる。全てのTCP-GW４０１～４０３に提供しても機能するが、効率は悪いし、セキュリティが破られる可能性も高くなる。これらの通信は、端末１０１、移動端末５０１、TCP-GW４０１、およびセキュリティサーバ６０１それぞれのセキュリティ情報管理１１２４、１５２４、１４２４、および１６２４の間で行われる。一旦、IPSec SAの情報がTCP-GW４０１に提供されれば、後の動作は（方式３）の場合と同様であるので省略する。

【００７６】

これから、移動端末（例えば移動端末５０１）の移動に伴いTCP-GWを変更するプロキシーハンドオフ制御について述べる。このため、移動端末５０１で終端される中継対象のTCPコネクション状態の情報と、移動端末５０１に対応するIPSec SA情報を、前のTCP-GW（例えばTCP-GW４０１）から後のTCP-GW（例えばTCP-GW４０２）に引き継ぐ必要がある。TCP-GW４０２は、移動端末５０１を起点・終点とする通信を検出した際に、前のTCP-GWを何らかの方法で探して、ハンドオフ処理を行うために必要な情報を要求する。このために予め隣接するTCP-GWをお互いに認識しておくことが有効である。

【００７７】

例えば、

（NR方式A）物理的な距離が近いTCP-GWを認識する、

（NR方式B）ネットワーク的な距離（ホップ数、遅延など）が近いTCP-GWを認識する、

といった方式が考えられる。

【００７８】

移動端末の物理的な移動によりハンドオフが必要になるとすると、（NR方式A）が望ましい。しかし、物理的な位置を知ることができない場合には、（NR方式B）を利用する場合もある。

【００７９】

（NR方式A）を実現するために、例えばプロキシ管理サーバ８０１を設ける。

TCP-GW４０１は基地局３０１と３０２、TCP-GW４０２は基地局３０３と３０４、TCP-GW４０３は基地局３０５と３０６の物理的な位置を何らかの方法で知りえており、その情報をプロキシ管理サーバ８０１に通知する。プロキシ管理サーバ８０１は、TCP-GW４０１と４０２の間のハンドオフ、TCP-GW４０２と４０３の間のハンドオフが発生し得ると判断する。そして、TCP-GW４０１に対してはTCP-GW４０２がハンドオフ対象となること、TCP-GW４０２に対してはTCP-GW４０１と４０３がハンドオフ対象となること、TCP-GW４０３に対してはTCP-GW４０２がハンドオフ対象となることを通知する。これらの処理は、TCP-GW４０１～４０３のTCPハンドオフ制御１４１０とプロキシ管理サーバ８０１によって行われる。もちろん、TCP-GW４０１～４０３に対して、これらの情報を手動で設定することも可能である。

【００８０】

また、（NR方式B）を実現するためには、例えば次のような手順が考えられる。

【００８１】

全てのTCP-GWが加入するマルチキャストグループを定義しておき、各TCP-GWのTCPハンドオフ制御１４１０がTTLを適当に制限したマルチキャストパケットを問い合わせするために送信する。これを受信した各TCPハンドオフ制御１４１０が送信元にユニキャストで応答することで、ホップ数の少ないTCP-GWを探すことができる。

【００８２】

さて、上述したように、端末１０１と移動端末５０１の間で、プロキシー介在を許容するIPSec SAの下で、TCP-GW４０１を介して、TCPによる通信を行っているとする。プロキシーハンドオフに伴う情報の引渡しにはいくつかのバリエーションが考えられる。

・ハンドオフする可能性のあるTCP-GWに、予め渡せる情報は渡しておくか否か。予め渡すとすれば以下のような候補がある。

【００８３】

－中継対象端末:新しいTCP-GWがこの端末の通信を検出した時に、どのTCP-G

Wに問い合わせれば、必要な情報が得られるかがわかる。

【００８４】

－IPSec SA情報:ハンドオフ遅延の減少が見込める。

・ユニキャストで問い合わせるか、マルチキャストで問い合わせるか。

【００８５】

－ユニキャスト:前のTCP-GWである可能性のある全てのTCP-GWに個別に問い合わせる。上記中継対象端末情報またはIPSec SA情報を持っていれば、その情報を提供したTCP-GWに問い合わせる。

【００８６】

－マルチキャスト: 前のTCP-GWである可能性のある全てのTCP-GWを含むマルチキャストグループを定義しておく。このマルチキャストグループ宛に問い合わせを送信する。

【００８７】

なお、ハンドオフに伴う通信は、原則としてセキュリティが確保された通信路によって行う。

【００８８】

ここで、TCP-GW４０１のセキュリティ情報管理１４２４から、TCP-GW４０２のセキュリティ情報管理１４２４に対して、予めIPSec SA情報が与えられているとする。TCP-GW４０１のセキュリティ情報管理１４２４は、セキュリティサーバ６０１から新たなIPSec SA情報を得ると、TCPハンドオフ制御１４１０に、そのIPSec SA情報を提供すべき先のTCP-GWを問い合わせる。この場合はTCP-GW４０２に提供するべきなので、TCP-GW４０１のセキュリティ情報管理１４２４は、TCP-GW４０２のセキュリティ情報管理１４２４に対して、そのIPSec SA情報を提供する。TCP-GW４０２のセキュリティ情報管理１４２４は、IPSec SA情報をSPDとSADに記憶すると共に、その提供元がTCP-GW４０１であることと、その提供時間を記憶する。

【００８９】

移動端末５０１が基地局３０１のエリアから、基地局３０２のエリアを経て、更に基地局３０３のエリアへ移動したとする。するとTCP-GW４０２が端末１０１

と移動端末５０１の間の通信を検出する。TCP-GW４０２のセキュリティ情報管理１４２４は、端末１０１と移動端末５０１の間のIPSec SA情報を、最近提供したものがTCP-GW４０１であることを認識するので、TCPハンドオフ制御１４１０に対して、TCP中継のハンドオフに必要な情報は、TCP-GW４０１から得られることを教える。また、TCP-GW４０２のセキュリティ情報管理１４２４は、TCP-GW４０３のセキュリティ情報管理１４２４に対して、対応するIPSec SA情報を通知する。以前から知っていたIPSec SA情報をこの時点で通知するのは、TCP-GW４０３へのハンドオフの可能性が生じたからである。

【００９０】

TCP-GW４０２のTCPハンドオフ制御１４１０は、TCP-GW４０１のTCPハンドオフ制御１４１０から得た、端末１０１と移動端末５０１間のTCPコネクションの情報から、TCP１４０１と無線TCP１４０３に対してTCP中継に必要な情報を設定する。例えば、シーケンス番号やウィンドウ制御関連の情報、設定されているTCPオプション、バッファに一時記憶されているデータパケットなどである。TCP中継の再開にあたっては、TCPシーケンス番号がなるべく乱れ無いように行う。つまり、バッファに一時記憶されているデータパケットのTCPシーケンス番号が、端末１０１と移動端末５０１の間を流れているTCPデータパケットのシーケンス番号よりも小さければ、それらを先に中継する。その後のTCP中継処理、およびIPSec関連の処理は既に述べた手順に準ずる。

【００９１】

次に、端末１０２がIPSecの機能を持たないIP端末で、ルータ７０１がセキュリティサービスとして、ネットワーク１０２からネットワーク２０１へ出る、IPSecで保護されていないパケットを、IPSecのトンネルモードで保護する場合について述べる。特に、カプセル化されたパケットをプロキシーで扱う方法について説明する。Mobile IPなど他のカプセル化の場合にも適用できる。

【００９２】

端末１０２と移動端末５０２の間の通信を想定する。移動端末５０２は、図４に構成を示すようなIPSec機能を持つ端末である。端末１０２は、図７に示すような構成でありIPSec機能を持たない端末である。この間で通信を行う際に、図

８に構成を示すルータ７０１と移動端末５０２の間でIPSecを利用した通信を行う。このため、既に述べたものと同様な方式で、ルータ７０１と移動端末５０２の間のIPSec SAが確立され、更にセキュリティサーバ６０１を介して、プロキシー介在を許容するIPSec SAの情報が必要なTCP-GW４０１に提供される。この際には、IPSecのトンネルモードが用いられる。端末１０２と移動端末５０２の間のパケットに対応するIPSecパケットは、図９（a）に示す形になる。

【００９３】

TCP-GW４０１での中継処理は既に述べた方法に準ずる。但し、セキュリティ情報管理１４２４の制御の下でIPSecを解いてカプセル化も外した後のパケットについては、IP入力部１４２３がTCP中継を行うか否かを判断し、必要な場合にTCP１４０１にパケットを渡すことになる。また、パケットを送信する際はIPSecとカプセル化の処理を行う（図９（ｂ）参照）。既に述べた方式との処理の切り替えは、SADから得たIPSec SA情報に含まれるIPSecプロトコルモードの値が、トランスポートモードであるか、トンネルモードであるかによって行うことができる。また、新しいIPヘッダが、カプセル化ヘッダであることを認識して行うこともできる。これは、例えばMobile IP（IETF RFC2002）によるHome AgentとForeign Agentの間のカプセル化されたTCP/IPパケットを扱うTCP-GWの場合など、一般にトンネルの中間にあるプロキシーの場合にも適用できる。

【００９４】

なお、上記の実施の形態はその主旨を逸脱しない範囲で種々変形して実施できることは言うまでもない。例えば、IPv6に適用することも可能である。

【００９５】

また、有線端末と無線端末の間だけではなく、無線端末５０１と無線端末５０８の間の通信にも本発明が適用できることは明らかである。

【００９６】

【発明の効果】

以上述べたような本発明によれば、IPSecなどでセキュリティを保証した通信に対しても、TCP-GWやSnoopに代表されるプロキシーを適用して無線環境下での性能の向上を図ることができる。

【図面の簡単な説明】

【図１】　本発明の中継装置、通信装置、制御装置を含んだネットワーク構成図。

【図２】　本発明のＴＣＰ－ＧＷのブロック構成図。

【図３】　本発明の端末のブロック構成図。

【図４】　本発明の移動端末のブロック構成図。

【図５】　本発明のセキュリティサーバのブロック構成図。

【図６】　本発明のIPSec処理前後のパケットフォーマットの構成図。

【図７】　本発明の別の端末のブロック構成図。

【図８】　本発明のルータのブロック構成図。

【図９】　本発明のIPSec処理前後のパケットフォーマットの構成図。

【符号の説明】

１０１、１０２、１０３　端末

２０１、２０２、２０３、２０４　ネットワーク

３０１、３０２、３０３、３０４、３０５、３０６　基地局

４０１、４０２、４０３　ＴＣＰ－ＧＷ

５０１、５０２、５０３、５０４、５０５、５０６、５０７、５０８　移動端末

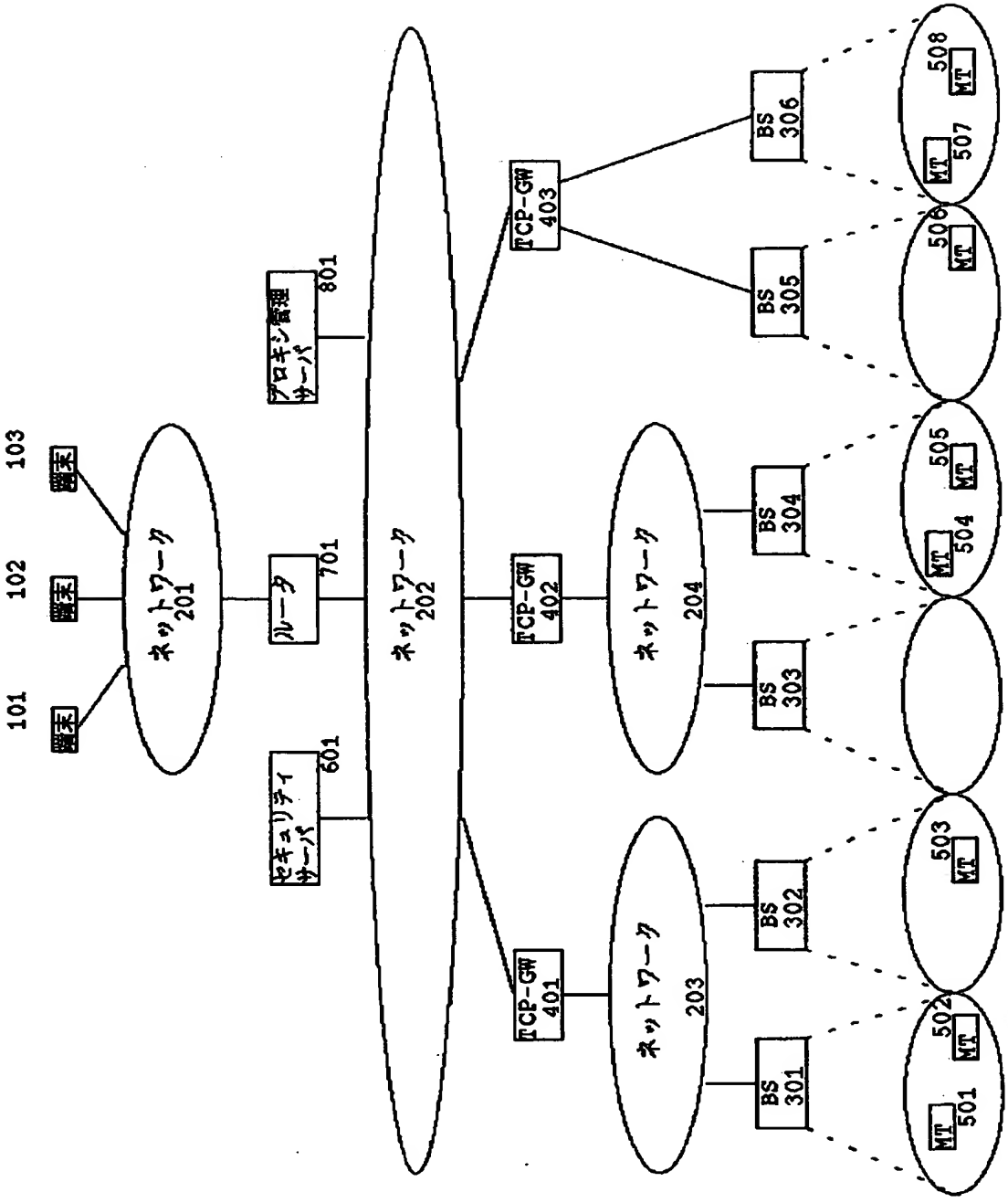
６０１　セキュリティサーバ

７０１　ルータ

８０１　プロキシ管理サーバ

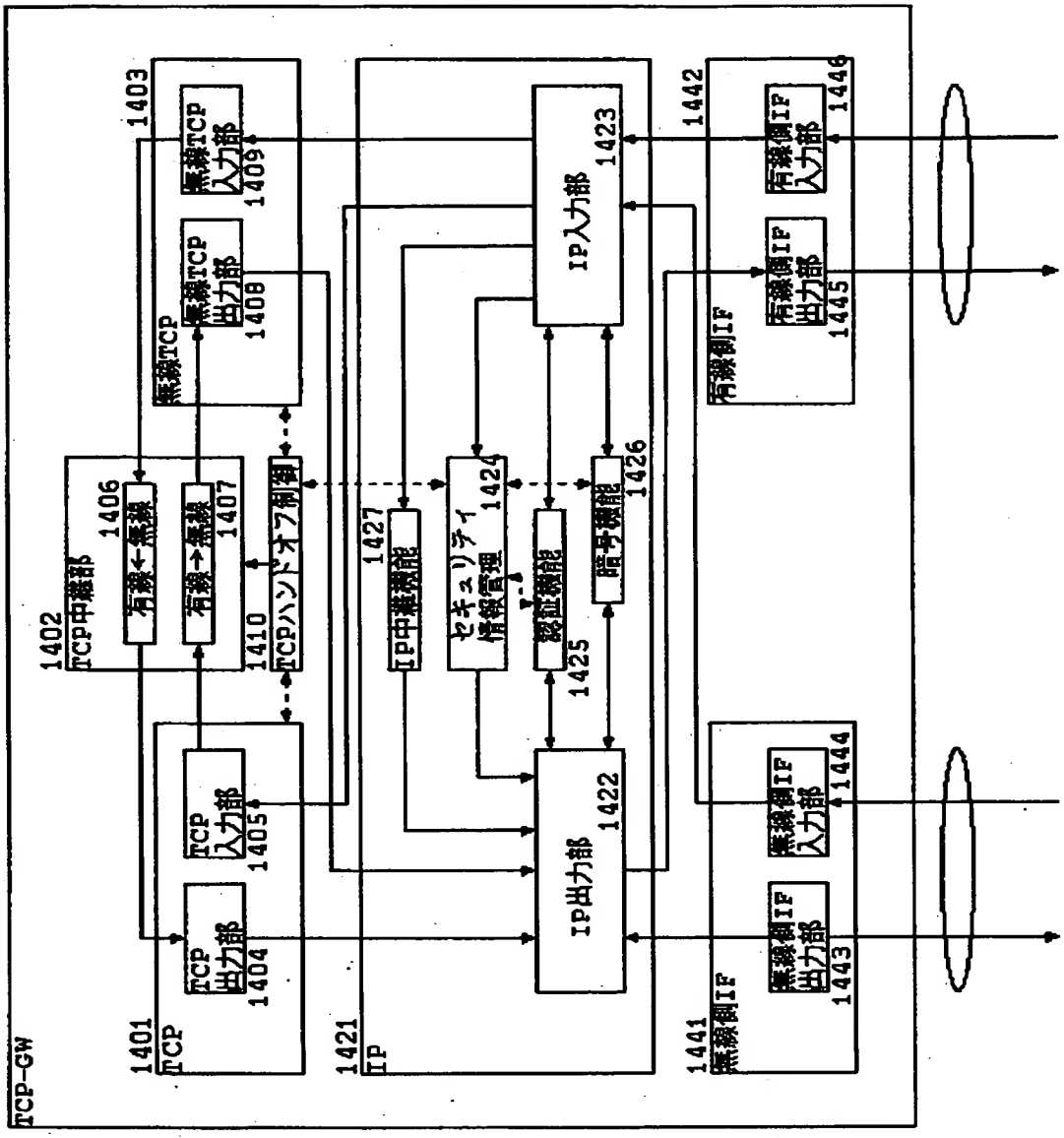
【書類名】　図面

【図１】

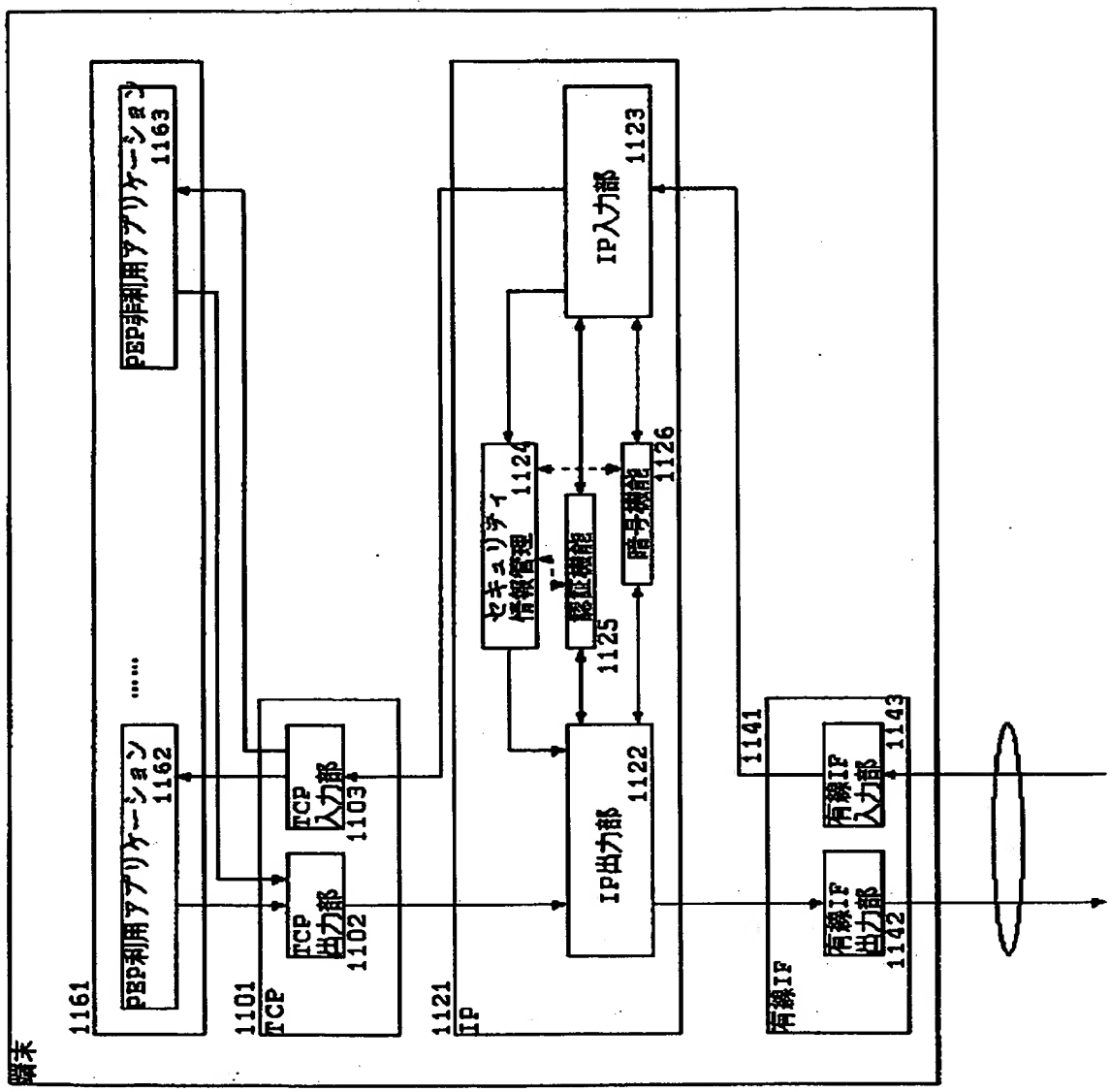


出証特２００１－３０４７４１６

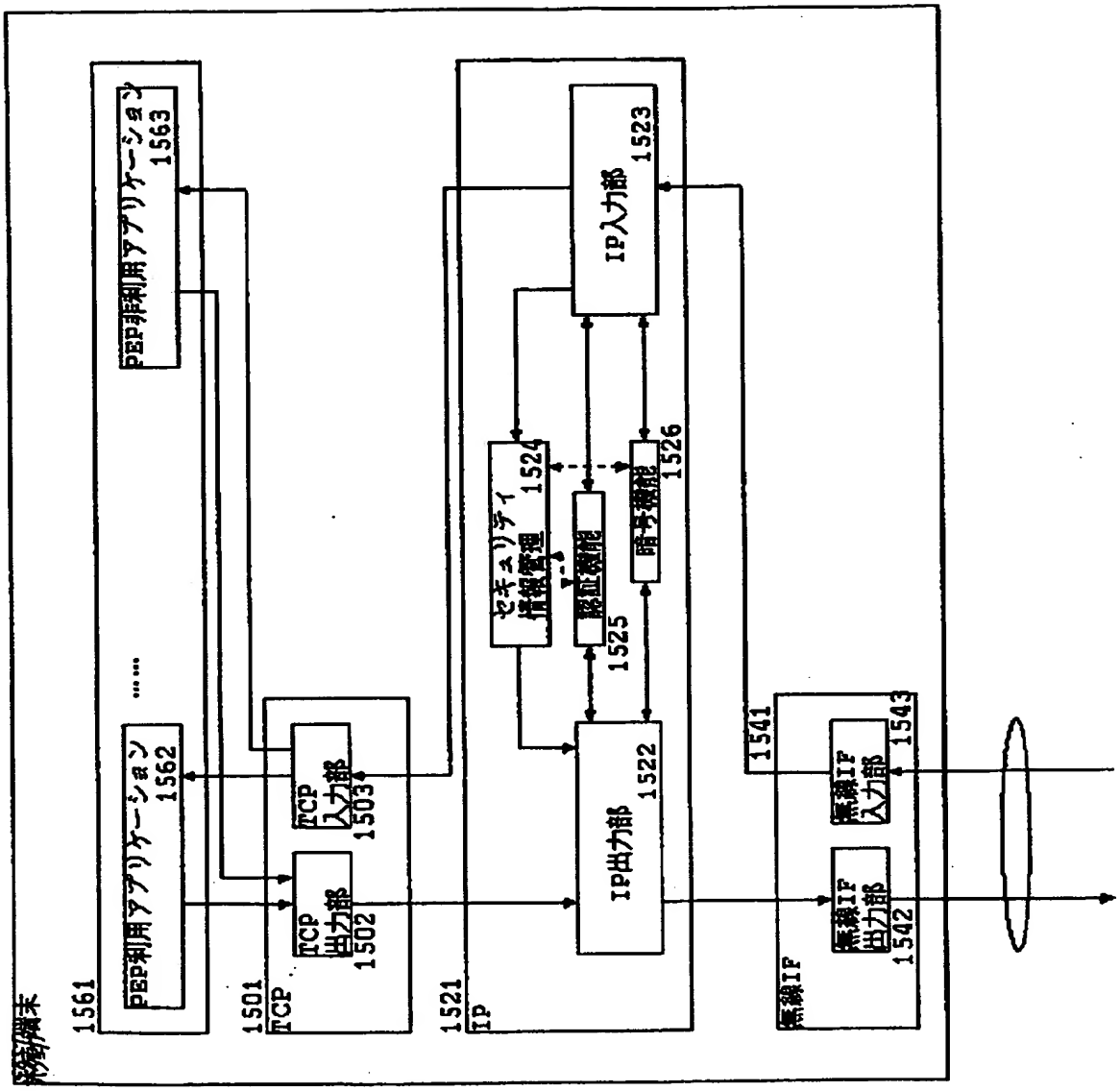
【図２】


TCP-GW
1401
TCP
1404
TCP出力部
1405
TCP入力部
1402
TCP中継部
1406
有線←無線
1407
有線→無線
1410
TCPハンドオフ制御
1403
無線TCP
1408
無線TCP出力部
1409
無線TCP入力部
1421
IP
1422
IP出力部
1423
IP入力部
1424
セキュリティ情報管理
1425
認証機能
1426
暗号機能
1427
IP中継機能
1441
無線側IF
1443
無線側IF出力部
1444
無線側IF入力部
1442
有線側IF
1445
有線側IF出力部
1446
有線側IF入力部

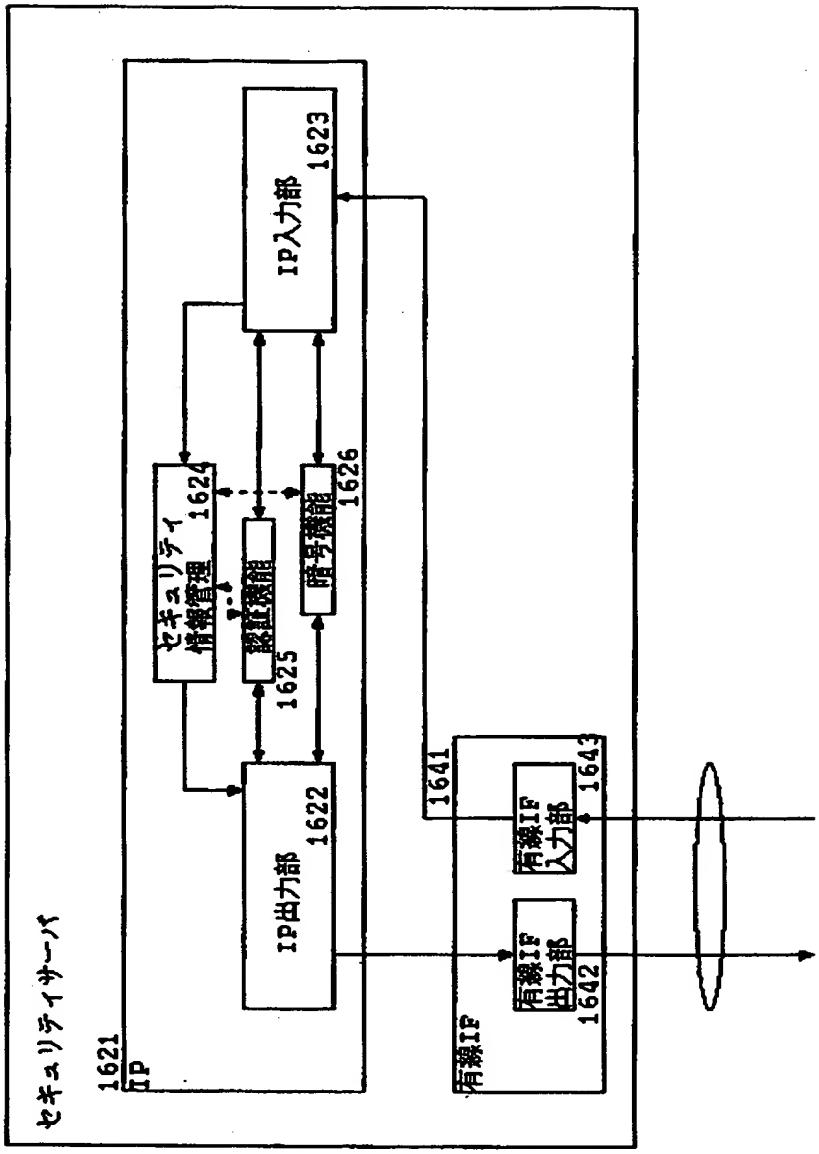
【図３】


端末
1161
PEP利用アプリケーション
1162
PEP利用アプリケーション
1163
1101
TCP
TCP
出力部
1102
TCP
入力部
1103
1121
IP
IP出力部
1122
IP入力部
1123
セキュリティ
情報管理
1124
認証機能
1125
暗号機能
1126
1141
有線IF
有線IF
出力部
1142
有線IF
入力部
1143

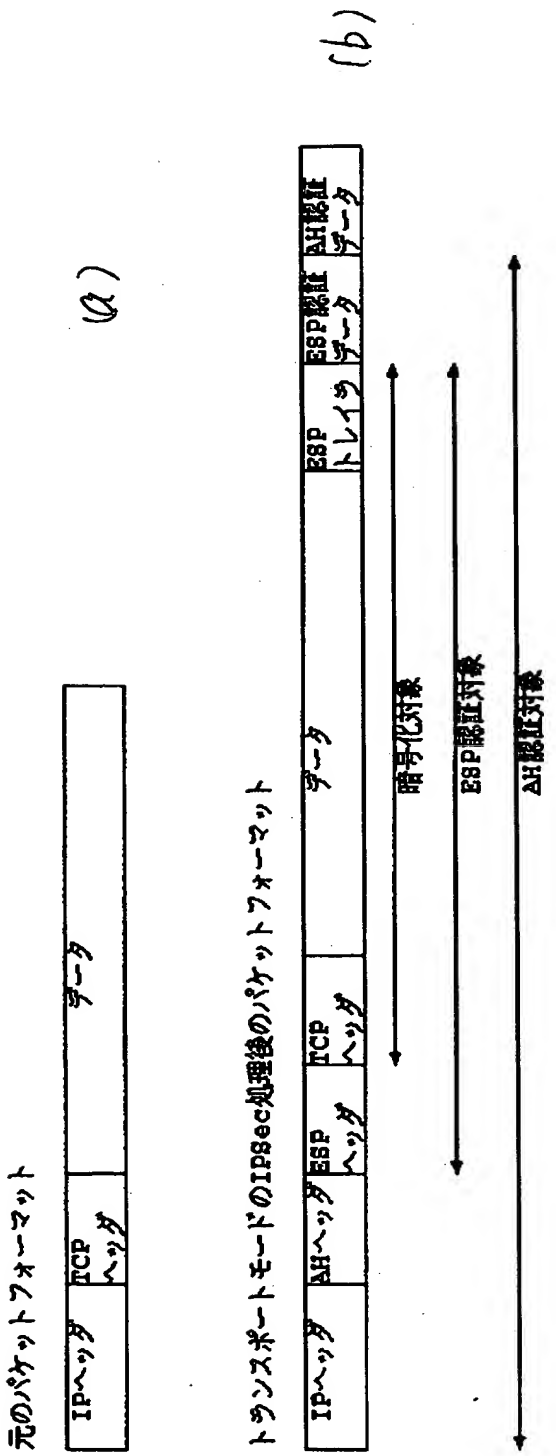
【図４】


移動端末
1561
PEP利用アプリケーション
1562
PEP非利用アプリケーション
1563
1501
TCP
TCP出力部
1502
TCP入力部
1503
1521
IP
IP出力部
1522
IP入力部
1523
セキュリティ情報管理
1524
認証機能
1525
暗号機能
1526
1541
無線IF
無線IF出力部
1542
無線IF入力部
1543

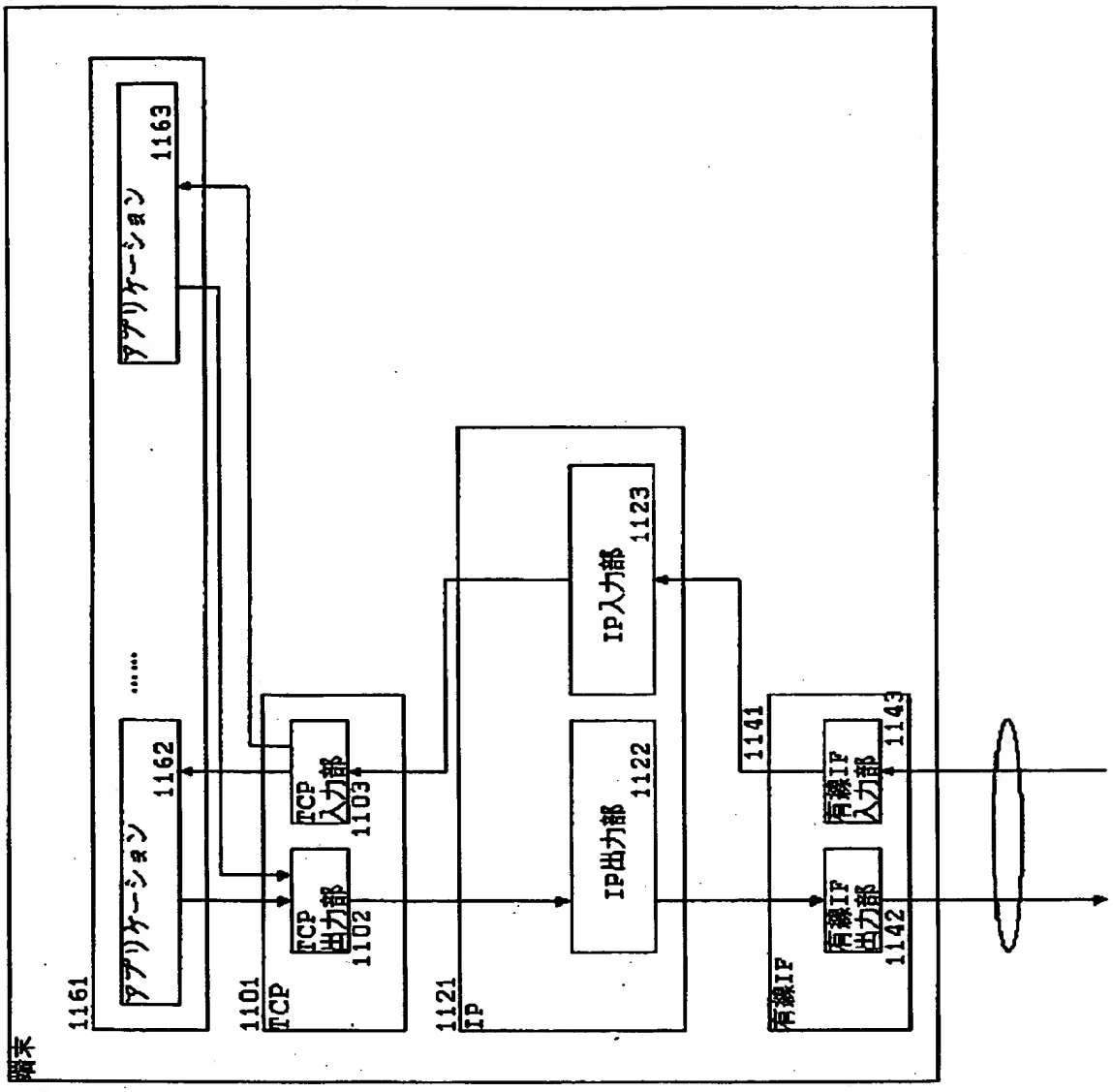
【図５】


セキュリティサーバ
1621
IP
IP入力部
1623
IP出力部
1622
セキュリティ情報管理
1624
認証機能
1625
暗号機能
1626
1641
有線IF
有線IF入力部
1643
有線IF出力部
1642

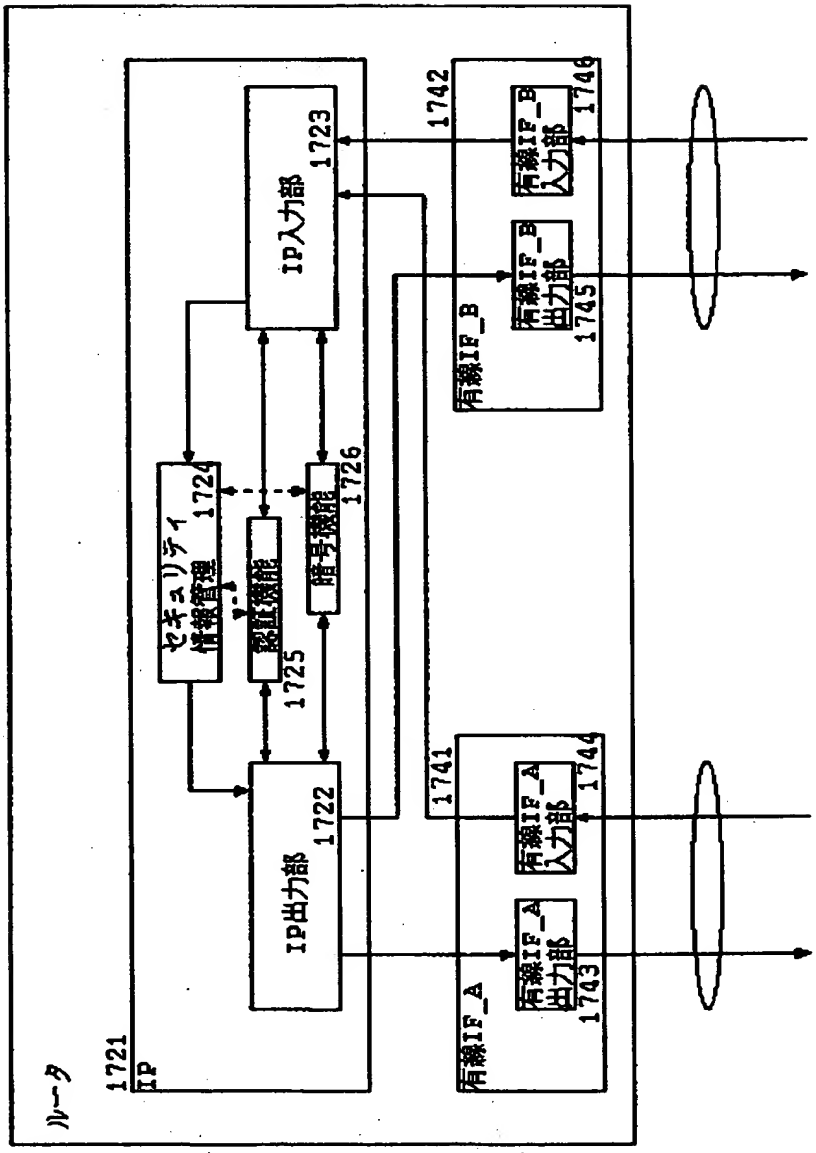
【図６】


(a)
(b)
元のパケットフォーマット
IPヘッダ
TCPヘッダ
データ
トランスポートモードのIPSec処理後のパケットフォーマット
IPヘッダ
AHヘッダ
ESPヘッダ
TCPヘッダ
データ
ESPトレイラ
ESP認証データ
AH認証データ
暗号化対象
ESP認証対象
AH認証対象

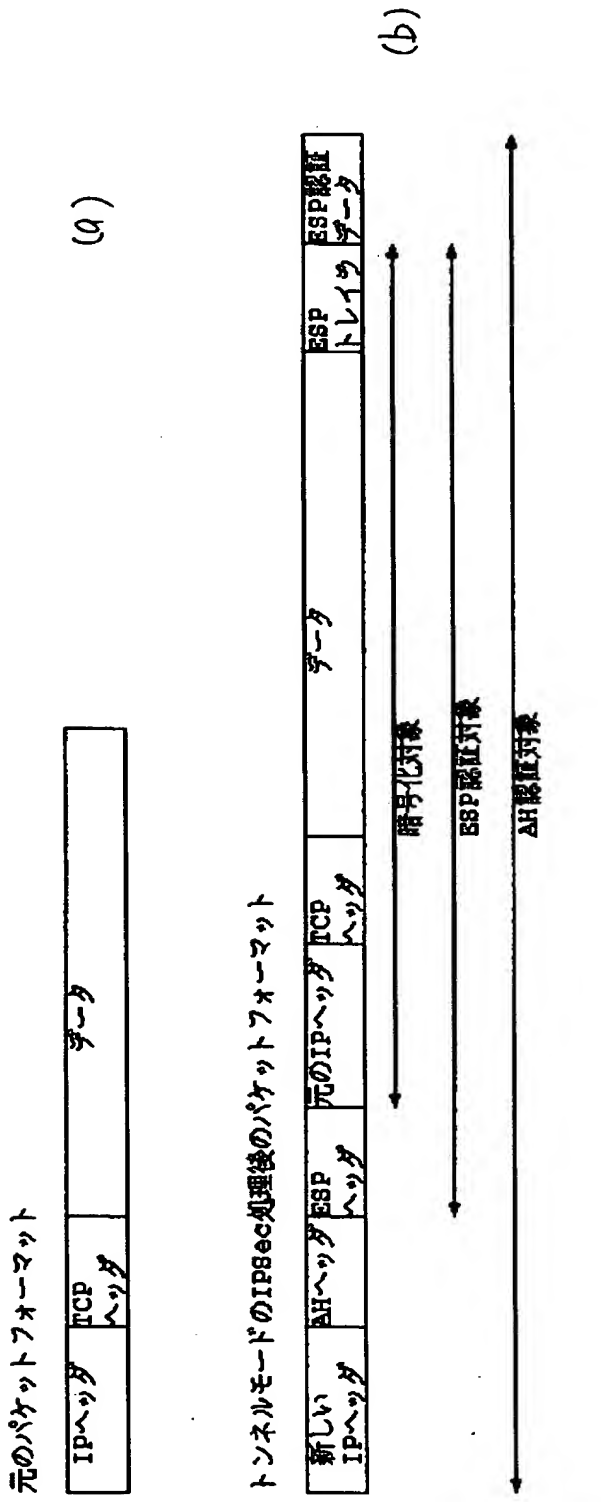
【図７】


端末
1161
アプリケーション
1163
アプリケーション
1162
.....
1101
TCP
TCP
出力部
1102
TCP
入力部
1103
1121
IP
IP出力部
1122
IP入力部
1123
1141
有線IF
有線IF
出力部
1142
有線IF
入力部
1143

【図８】


ルータ
1721
IP
IP入力部
1723
IP出力部
1722
セキュリティ情報管理
1724
認証機能
1725
暗号機能
1726
1741
1742
有線IF_A
有線IF_B
有線IF_A 出力部
1743
有線IF_A 入力部
1744
有線IF_B 出力部
1745
有線IF_B 入力部
1746

【図９】


(a)
元のパケットフォーマット
IPヘッダ
TCPヘッダ
データ
(b)
トンネルモードのIPSec処理後のパケットフォーマット
新しいIPヘッダ
AHヘッダ
ESPヘッダ
元のIPヘッダ
TCPヘッダ
データ
ESPトレイラ
ESP認証データ
暗号化対象
ESP認証対象
AH認証対象

【書類名】　要約書

【要約】

【課題】　セキュリティを維持しつつ、無線端末装置と有線端末装置間で通信を行う中継装置、通信装置、制御装置および通信制御方法の提供。

【解決手段】　ネットワーク２０１はTCP/IP端末１０１～１０３を収容し、IPパケットを交換するルータ７０１によってネットワーク２０２と相互接続される。ネットワーク２０２はTCP-GW４０１と４０２とによってネットワーク２０３、２０４を、TCP-GW４０３によって基地局３０５と３０６を収容する。ネットワーク２０２はセキュリティサーバ６０１を持つ。ネットワーク２０３と２０４は、それぞれ基地局３０１と３０２、基地局３０３と３０４を収容する。基地局３０１には移動端末５０１と５０２、基地局３０２には移動端末５０３、基地局３０４には移動端末５０４と５０５、基地局３０５には移動端末５０６、そして基地局３０６には移動端末５０７と５０８が存在する。移動端末５０１～５０８はTCP/IP端末である。

【選択図】　図１

出 願 人 履 歴 情 報

識別番号　〔０００００３０７８〕

１．変更年月日　１９９０年　８月２２日
［変更理由］　新規登録
住　所　神奈川県川崎市幸区堀川町７２番地
氏　名　株式会社東芝